REMARKS

Currently, claims 4 to 7 are pending in the present application.

Applicants respectfully request reconsideration of the present application in view of this response.

Claims 4 to 7 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 4,868,877 to Fischer (the "Fischer reference").

As discussed in Applicants' earlier Response, the Fischer reference purportedly concerns a public key cryptographic system with enhanced digital signature certification, employing a hierarchy of nested certifications and signatures which indicate the authority and responsibility levels of the individual whose signature is being certified. Abstract, lines 1-6.

Independent claim 4 of the present application concerns a method for generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location correspondence to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center.

In contrast, the Fischer reference does not *identically* disclose (as it must for anticipation) or suggest at least the features of *producing the at least one encryption key pair* including a public part and a secret part; *marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair*; after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center; unequivocally assigning the at least one encryption key pair to the user; *causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair*; after the check of the unequivocal assignment is performed successfully, *causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair*; *encrypting the new certificate using the public part of the at least one encryption key pair*, as claimed in claim 4. Instead, the Fischer reference refers to a user digitally signing a purchase order under the authority of a certificate appended to the transmitted message – a message can be signed by applying to it at least a portion of the object being signed, the privately held signature key. Col. 7, lines 5-11. The Fischer reference further states that by

signing an image of the object or a more compact version thereof known as a digest or hash of the object, with the secret key, it is possible for anyone with access to the public key to encrypt the result and compare it with the object or a recomputed hash or digit version thereof. Col. 7, lines 11-17. The Fischer reference further states that because only the owner of the public key could have used the secret key to perform this operation, the owner of the public key is thereby confirmed to have signed the message. Col. 7, lines 17-20. The Fischer reference states that a digital signature is accompanied by at least one valid certificate which specifies the identity of the signer and the authorization which the signer has been granted – to be valid, a certificate must be signed by the private key associated with one or more other valid certificates. Col. 7, lines 20-33. The Fischer reference indicates that one or more other valid certificates must grant the signer the authority to create such a signature and/or to issue the purchase order. Col. 7, lines 33-36. The Fischer reference further states that any party who receives a message transmitted by the user can verify and validate the user's signature and the authority that the user exercised, such validation being possible since a complete hierarchy of validating certificates is transmitted with the original purchase order which permits the ultimate recipient to feel confident that the requested transaction is authentic and properly authorized. Col. 7, line 61 - col. 8, line 3.

In Further Response

The Office Action states that col. 6, lines 14-16, and col. 8, lines 4-16, of the Fischer reference show elements of the present claim 4. The Fischer reference at col. 6, line 14-16, recites that each terminal user has a *public encrypting key* and an associated *private secret decrypting* key. ***In contrast***, claim 4 of the present application requires producing the at least one *encryption key pair* including a public part and a secret part; *marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair*; after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center; and *unequivocally assigning the at least one encryption key pair to the user*. The Fischer reference at col. 8, lines 4-16, recites that a corporate organization participating in a public key cryptosystem registers a set of public keys (which they are authorized to use) with a meta-certifier. The Fischer reference at col. 8, lines 16-24, further explains that these public keys are "'high

level' keys" to be used for certifying the organization's personnel; the meta-certifier distributes to the organization its certification that each of the supplied public keys is authorized for the organization's use – in effect, the meta-certifier certifies that the party using each key is actually associated with the organization. The Fischer reference at col. 8, lines 24-27, recites that the meta-certifier's certification may include embedded text which indicates that the users of registered public keys are properly associated with the organization. ***In contrast***, claim 4 of the present application requires unequivocally assigning the at least one encryption key pair to the user; causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair; after the check of the unequivocal assignment is performed successfully, *causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair*; *encrypting the new certificate using the public part of the at least one encryption key pair*; and causing the trust center to transmit the encrypted new certificate to the user.

Accordingly, the Fischer reference does not render obvious claim 4, and withdrawal of the rejection of claim 4 under 35 U.S.C. § 102 (b) is respectfully requested.

Since claims 5 and 6 depend from claim 4, claims 5 and 6 are allowable for at least the same reasons as claim 4. Claim 7 recites features analogous to those of claim 4 and is allowable for essentially the same reasons as claim 4.

Accordingly, the Fischer reference does not identically disclose or even suggest the features of claim 4. Thus, withdrawal of the rejection of claims 4 to 7 under 35 U.S.C. § 102(b) is respectfully requested.

In summary, it is respectfully submitted that all of claims 4 to 7 of the above-identified application are allowable for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that the rejections of claims 4 to 7 have been obviated and all claims 4 to 7 are allowable.

It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

If it would further allowance of the present application, the Examiner is invited to contact the undersigned.

Respectfully submitted,

By: Quick Study
Reg. No. 47084

Dated: June 9, 2004

By: Richard L. Mayer
Richard L. Mayer
(Reg. No. 22,490)

CUSTOMER NO. 26646

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200